# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-222622
(43)Date of publication of application : 17.08.2001

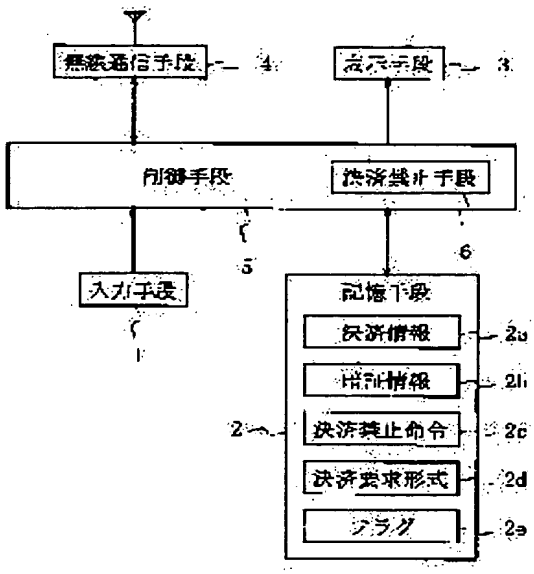
(51)Int.Cl. G06F 17/60
G07F 19/00
G07F 7/08
G07F 7/12
G07G 1/12
G07G 1/14

(21)Application number : 2000-035700
(22)Date of filing : 08.02.2000

(71)Applicant : FUTURE FINANCIAL STRATEGY KK
FUTURE SYSTEM CONSULTING CORP
(72)Inventor : TOGASHI NAOKI

## (54) COMMUNICATION DEVICE WITH SETTLEMENT FUNCTION

(57)Abstract:
PROBLEM TO BE SOLVED: To conduct settlement similar to conventional credit card settlement and Debit card settlement without passing a card to a storeclerk.
SOLUTION: This device is equipped with an input means 1 for information, a storage means 2 for information, a display means 3 for information, a communication means 4 which sends and receives information to and from an external device, and a control means 5 which associates them to enable a communication of information. Further, the device is equipped with a settlement information storage means 2a stored with settlement information corresponding to a credit card number, etc., and a password code information storage means 2b stored with a password code information. The control means 5 is equipped with a settlement function of inputting password code information from the input means 1 and a settlement request, matching the password code information received from the input means 1 against the password code information stored in the password code information storage means 2b, reading settlement information out of the settlement information storage means 2a in response to the input of the settlement request when the both match each other, and sending the settlement information to the external device through the communication means 4.




## LEGAL STATUS

[Date of request for examination] 28.04.2000
[Date of sending the examiner's decision of rejection] 03.09.2002
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]

[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－222622
（P2001－222622A）
(43)公開日　平成13年８月17日(2001.8.17)

| (51)Int.Cl.⁷ | 識別記号 | ＦＩ | | テーマコード（参考） |
|---|---|---|---|---|
| Ｇ０６Ｆ　17/60 | | Ｇ０７Ｇ　1/12 | ３２１Ｐ | ３Ｅ０４０ |
| Ｇ０７Ｆ　19/00 | | 1/14 | | ３Ｅ０４２ |
| 7/08 | | Ｇ０６Ｆ　15/21 | ３４０Ａ | ３Ｅ０４４ |
| 7/12 | | Ｇ０７Ｄ　9/00 | ４７６ | ５Ｂ０４９ |
| Ｇ０７Ｇ　1/12 | ３２１ | Ｇ０７Ｆ　7/08 | Ｒ | |

審査請求　有　請求項の数４　ＯＬ　（全６頁）　最終頁に続く

(21)出願番号　特願2000－35700(P2000－35700)

(22)出願日　平成12年２月８日(2000.2.8)

(71)出願人　500049484
フューチャーフィナンシャルストラテジー株式会社
東京都渋谷区渋谷三丁目28番13号　渋谷新南口ビル

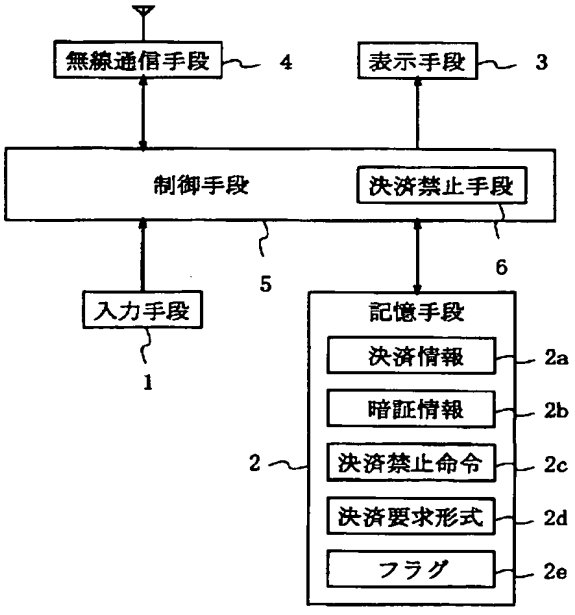
(71)出願人　399059049
フューチャーシステムコンサルティング株式会社
東京都渋谷区渋谷三丁目28番13号　渋谷新南口ビル

(74)代理人　100110652
弁理士　塩野谷　英城

最終頁に続く

(54)【発明の名称】　決済機能付き通信装置

(57)【要約】
【課題】　従来のクレジットカード決済やデビットカード決済と同様の決済を店員にカードを手渡すことなく行えるようにすること等。
【解決手段】　情報の入力手段１と、情報の記憶手段２と、情報の表示手段３と、外部装置との間で情報の送受を行う通信手段４と、これらを連係させ情報の通信を可能とする制御手段５とを備える。また、クレジットカード番号等に相当する決済情報を記憶した決済情報記憶手段２ａと、暗証情報を記憶した暗証情報記憶手段２ｂとを備える。制御手段５は、入力手段１から暗証情報の入力と決済要求の入力とを受け付け、入力手段１から受け付けた暗証情報を暗証情報記憶手段２ｂに記憶されている暗証情報と照合し、両者が一致した場合、決済要求の入力に応答して決済情報記憶手段２ａから決済情報を読み出し当該決済情報を通信手段４を介して外部装置に送信する決済機能を備えている。



1

【特許請求の範囲】

【請求項１】　情報の入力手段と、情報の記憶手段と、情報の表示手段と、外部装置との間で情報の送受を行う通信手段と、これらを連係させ情報の通信を可能とする制御手段とを備えた決済機能付き通信装置において、

クレジットカード番号等に相当する決済情報を記憶した決済情報記憶手段と、暗証情報を記憶した暗証情報記憶手段とを備え、

前記制御手段は、前記入力手段から暗証情報の入力と決済要求の入力とを受け付け、前記入力手段から受け付けた暗証情報を暗証情報記憶手段に記憶されている暗証情報と照合し、両者が一致した場合、前記決済要求の入力に応答して前記決済情報記憶手段から決済情報を読み出し当該決済情報を前記通信手段を介して外部装置に送信する決済機能を備えていることを特徴とした決済機能付き通信装置。

【請求項２】　前記制御手段は、前記決済情報を前記表示手段に表示しないことを特徴とした請求項１記載の決済機能付き通信装置。

【請求項３】　請求項１記載の決済機能付き通信装置において、

決済禁止命令を記憶した決済禁止命令記憶手段と、制御手段の制御により少なくとも前記決済情報の送信を禁止する決済禁止手段とを備え、

前記制御手段は、前記通信手段を介して受信した情報を前記決済禁止命令記憶手段に記憶された決済禁止命令と照合し、両者が一致した場合、前記決済禁止手段を起動することを特徴とした決済機能付き通信装置。

【請求項４】　前記通信手段は、無線による通信手段であることを特徴とした請求項１記載の決済機能付き通信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、決済機能付き通信装置に係り、特に、携帯電話やページャー等の通信装置に決済機能を持たせたものに関する。

【０００２】

【従来の技術】従来、商取引の決済にクレジットカードが一般的に用いられている。

【０００３】

【発明が解決しようとする課題】しかしながら、上記従来例にあっては、決済の際にクレジットカードを店員に手渡す必要があり、カードに記録された情報が盗まれるおそれがあった。また、カード会社は、会員にカードを郵送する手間があった。また、会員はカードを紛失した際、カード会社のコールセンターに連絡を取ってカードの使用を差し止めてもらう手間があった。また、カード会社のコールセンターは、カードを紛失した会員の対応に追われる手間があった。

【０００４】

2

【発明の目的】本発明は、かかる従来例の有する不都合を改善し、特に、従来のクレジットカード決済やデビットカード決済と同様の決済を店員にカードを手渡すことなく行えるようにする。また、カード会社が会員にクレジットカードを発送する手間を不要とする。また、カードを紛失した会員がコールセンターにカードの使用禁止を申し立てる手間を不要とする。また、カード会社がカードを紛失した会員から依頼を受けてカードの使用を禁止する手間を不要とする。

【０００５】

【課題を解決するための手段】上記目的を達成するため、請求項１記載の発明は、情報の入力手段と、情報の記憶手段と、情報の表示手段と、外部装置との間で情報の送受を行う通信手段と、これらを連係させ情報の通信を可能とする制御手段とを備えている。また、クレジットカード番号に相当する決済情報を記憶した決済情報記憶手段と、暗証情報を記憶した暗証情報記憶手段とを備えている。そして、制御手段は、入力手段から暗証情報の入力と決済要求の入力とを受け付け、入力手段から受け付けた暗証情報を暗証情報記憶手段に記憶されている暗証情報と照合し、両者が一致した場合、決済要求の入力に応答して決済情報記憶手段から決済情報を読み出し当該決済情報を通信手段を介して外部装置に送信する決済機能を備えている、という構成を採っている。

【０００６】ここで、決済情報には、クレジットカード番号に相当する番号やデビットカードの口座番号に相当する番号等が含まれる。本発明では、ユーザーは、例えば買い物の際にレジに備え付けられたＰＯＳ等の店頭装置の前で、本願装置の入力手段から自己の暗証番号と決済要求とを入力する。正しい暗証番号が入力されれば、従来のクレジットカード番号に相当する決済情報が通信手段から店頭装置に送信され、店頭装置では、この決済情報を受信し、従来カードリーダで読み取っていた決済情報と同様に扱って決済処理を完了する。

【０００７】請求項２記載の発明では、制御手段は、決済情報を前記表示手段に表示しない、という構成を採っている。本発明では、本願の決済機能付き通信装置に格納された決済情報を当該装置の外部から確認できない。

【０００８】請求項３記載の発明では、請求項１記載の決済機能付き通信装置において、決済禁止命令を記憶した決済禁止命令記憶手段と、制御手段の制御により少なくとも決済情報の送信を禁止する決済禁止手段とを備える。そして、制御手段は、通信手段を介して受信した情報を決済禁止命令記憶手段に記憶された決済禁止命令と照合し、両者が一致した場合、決済禁止手段を起動する、という構成を採っている。

【０００９】決済禁止手段としては、例えば次のような構成が考えられる。

（１）制御手段のソフトウェア処理により記憶手段に決済禁止を示すフラグを立て、当該フラグが立っている間

は制御手段が決済要求の入力を無視するもの。
（２）制御手段のソフトウェア処理により記憶手段に使用拒否を示すフラグを立て、当該フラグが立っている間は制御手段が装置電源を切断し、かつ、装置電源の投入操作を無視するもの（物理的なスイッチングを操作不能とするものを含む）。
（３）制御手段のソフトウェア処理により決済情報又は／及び暗証番号を記憶手段から消去してしまうもの。
（４）決済情報の送信に必要な電子回路（素子及び配線を含む）の一部を過電流や外圧等により物理的に破壊するもの。
【００１０】本発明では、本願装置を紛失したことに気付いたユーザーは、例えば最寄りの電話端末から通信網を介して本願装置に接続し、例えばトーン信号により決済禁止命令を本願装置に伝達する。この決済禁止命令を受信した制御手段は、例えば上記のような決済禁止手段を起動することにより、以降の決済情報の送信を禁止する。
【００１１】また、請求項４記載の発明では、通信手段は、無線による通信手段である、という構成を採っている。これにより、前述した目的を達成しようとするものである。
【００１２】
【発明の実施の形態】以下、本発明の一実施形態を図１及び図３に基づいて説明する。
【００１３】図１は、本発明の決済機能付き通信装置を組み込んだ携帯電話装置のブロック図である。ただし、本願装置は、携帯電話装置に搭載できるほか、本願装置単体でも機能するものであり、また、ページャー等への搭載も可能である。
【００１４】図１に示す携帯電話装置は、情報の入力手段１と、情報の記憶手段２と、情報の表示手段３と、無線で情報の送受を行う無線通信手段４と、これらを連係させ情報の無線通信を可能とする制御手段５とを備えている。また、クレジットカード番号に相当する決済情報を記憶した決済情報記憶手段２ａと、暗証情報を記憶した暗証情報記憶手段２ｂとを備えている。制御手段５は、入力手段１から暗証情報の入力と決済要求の入力とを受け付け、入力手段１から受け付けた暗証情報を暗証情報記憶手段２ｂに記憶されている暗証情報と照合し、両者が一致した場合、決済要求の入力に応答して決済情報記憶手段２ａから決済情報を読み出し当該決済情報を無線通信手段４を介して外部装置に送信する決済機能を備えている。
【００１５】また本実施形態において、図１に示す携帯電話装置は、決済禁止命令を記憶した決済禁止命令記憶手段２ｃと、制御手段５の制御により少なくとも決済情報の送信を禁止する決済禁止手段６とを備えている。制御手段５は、無線通信手段４を介して受信した情報を決済禁止命令記憶手段２ｃに記憶された決済禁止命令と照合し、両者が一致した場合、決済禁止手段６を起動するようになっている。
【００１６】これを更に詳述すると、本実施形態において、入力手段１は、テンキー等を備えた操作盤である。記憶手段２は、ＲＡＭやＲＯＭ（書き換え可能なＲＯＭを含む）である。決済情報記憶手段２ａ、暗証情報記憶手段２ｂ、決済禁止命令記憶手段２ｃ、決済要求形式記憶手段２ｄ及びフラグ記憶手段２ｅは、記憶手段２の記憶領域である。決済情報２ａは、既存のクレジットカード番号に相当する例えば１６桁の番号情報を含んでいる。暗証情報２ｂは、例えば４桁の所定の番号で構成された情報である。決済禁止命令２ｃは、外部の電話端末から入力可能な所定のデータ列から構成される。決済要求形式２ｄは、所定のキー入力に対応する情報（例えば「＊」「１」等）を予め定義したものである。フラグ２ｅは、決済禁止手段６の処理に用いられる。制御手段５は、決済情報２ａを表示手段３に表示しないようになっている。決済情報及び暗証情報は、オンラインで取得し記憶手段２に格納するようにしてもよい。
【００１７】また、表示手段３は、例えば液晶表示盤である。無線通信手段４は、ＲＦ部、ベースバンド部、マイク及びスピーカ等を含んで構成され、屋内通信機能（例えばbluetooth通信機能）と屋外通信機能（外線発着信機能）との双方を備えている。制御手段５は、コンピュータ及び各手段１～４に対応したインターフェースを含んでいる。決済禁止手段６は、制御手段５のプログラム処理により記憶手段２に決済禁止を示すフラグ２ｅを立て、当該フラグ２ｅが立っている間は制御手段５が決済要求の入力を無視するものである。
【００１８】次に、本実施形態の動作を図２及び図３に基づいて説明する。
【００１９】本実施形態は、通常の携帯電話としての使用に加え、従来のクレジットカード決済においてクレジットカードの代替として使用することができるバーチャルクレジットカード機能を実現する。
【００２０】図２は、バーチャルクレジットカードを実現するフローチャートである。
【００２１】携帯電話の所有者は、店舗で例えば買い物を済ませ、レジで精算を行う。店員から決済を求められると、購入者は携帯電話を操作し、まず入力手段１から暗証情報を入力し、続いて決済要求を示すキー入力（例えば「＊」「１」）を行う（Ｓ１）。
【００２２】制御手段５は、入力手段１から入力された情報を決済要求形式２ｄに照合し、決済要求であることを確認すると（Ｓ２）、続いて入力手段１から入力された暗証情報を記憶手段２に格納された暗証情報２ｂに照合する（Ｓ３）。この結果、暗証情報が一致すると、制御手段５は、記憶手段２のフラグ２ｅがオンになっているか確認する（Ｓ４）。この結果、フラグ２ｅがオフであれば、制御手段５は、決済情報２ａを記憶手段２から

読み出し、無線通信手段４の屋内通信機能を起動して決済情報２ａを店舗のＰＯＳ端末等の店舗装置に送信する（Ｓ５）。この際、制御手段５は、決済情報を表示手段３に表示しない。店舗装置は、屋内通信機能を備え、購入者の携帯電話から送信された決済情報を受信し記憶手段に格納する。その後、店舗装置は、当該決済情報を従来のカードリーダによりクレジットカードから読み取った決済情報と同様に取り扱い、商取引の決済を完了する。一方、Ｓ２で決済要求と認められない場合、Ｓ３で暗証情報が正しくない場合、Ｓ４でフラグがオンの場合は、いずれも決済情報を送信せずに処理をエラー終了する。この際、制御手段５は、エラー終了の理由を表示手段３に表示しない。

【００２３】図３は、携帯電話の盗難に対処する処理を示したフローチャートである。

【００２４】携帯電話の紛失に気付いたユーザは、最寄りの電話端末等から紛失した携帯電話宛に発信し、呼を接続する。続いて、ユーザは例えば電話端末のプッシュボタンを用いて暗証情報と所定の決済禁止命令を入力する。一方、携帯電話の制御手段５は、着信後に受信した情報を記憶手段２の暗証情報２ｂに照合し（Ｓ１１，Ｓ１２）、暗証情報の一致が確認されると、続いて、受信した情報を決済禁止命令２ｃに照合する（Ｓ１３）。この結果、決済禁止命令であると判断すると、決済禁止手段６を起動し、記憶手段２のフラグ２ｅをオンにする（Ｓ１４）。これにより、図２のＳ４の判断で決済処理はエラー終了するため、以降決済情報の送信は行われず、紛失した携帯電話のバーチャルクレジットカードが不正使用される事態を防止できる。また、紛失した携帯電話が発見された場合、制御手段５が予め定義された所定の操作を入力手段１から受け付けることにより、記憶手段２のフラグをオフし、再度決済機能を復活させる機能を備えていてもよい。

【００２５】以上説明した本実施形態によれば、決済の際にクレジットカードを店員に手渡す必要がないので、従来のようにカードに記録された情報が盗まれるおそれが少ない。また、決済情報及び暗証情報を予め記憶させるか又はオンラインで取得させることにより、カード会社は、ユーザにカードを郵送する手間が不要となる。また、決済禁止機能を搭載したので、ユーザは、従来のカード会社のコールセンターに頼らずに、自分で速やかに決済機能の差し止めができ、コールセンターに連絡を取る手間が不要になると共に、従来より速やかな差し止めが可能となり、不正使用に対する安全性が高まる。また、カード会社のコールセンターは、カードを紛失した会員の対応に追われる手間が不要となり、費用削減を図ることができる。

【００２６】しかしながら、携帯電話の電源がオフされている場合は、当該携帯電話に着信することができず、上記決済禁止機能を有効に機能させることが出来ない。そこで、携帯電話が決済の際に外線発信を用いる場合、中継所となる電話会社のコールセンターのコンピュータに使用可否のフラグを予め設け、当該センターのコンピュータは、携帯電話からの発信を受信した時、当該携帯電話に対応する使用可否のフラグの設定を確認し（携帯電話に対応するフラグの判別は、例えば発信者番号に基づいて行うことができる。）、当該使用可否フラグの設定が使用不可に設定されている場合は、当該携帯電話の使用を禁止する。この使用可否のフラグは、携帯電話の正規の所有者が最寄りの電話からセンターのコンピュータに接続し、携帯電話を特定する情報（携帯電話の発信者番号等）の入力と所定のパスワードの入力とを行うことによって設定変更できるように構成する。このようにすると、盗難にあった携帯電話の電源がオフになっているときでも、正規の所有者はセンターのコンピュータに接続することにより、使用可否フラグの設定を使用不可に設定することができ、その後は、盗難された携帯電話から送信される決済情報による決済を確実に禁止することができる。

【００２７】ここで、本発明は上記実施形態に限定されない。例えば、決済要求と暗証情報の入力順序や入力タイミング等は適宜設計変更されてもよい。また、決済禁止手段の構成は、上述のように種々考えられるし、決済機能の禁止に限らず他の携帯電話としての機能を使用禁止することもできる。また、本願の決済機能付き通信装置は、上述のように携帯電話への搭載に限らず、決済専用装置としての実現やページャー等の他の通信装置への搭載も可能である。また、店舗装置との通信は、電波による通信に限らず赤外線通信等でもよい。また、店舗装置との通信は、無線に限らず有線通信の場合も考えられる。また、上記実施形態では、決済情報として、従来のクレジットカード番号に相当する番号を記憶したバーチャルクレジットカードの構成を示したが、決済情報としてデビットカードの口座番号に相当する番号を記憶させたバーチャルデビットカードの実現も可能である。また、上記実施形態において、制御手段５は、入力手段１から支払方法（１回払い、１ヶ月後等のスキップ払い、ボーナス払い、リボ払い（複数回払い）など）の選択入力を受け付け、この支払方法の情報を店舗装置に送信するようにしてもよい。店舗装置は、受信した支払方法の情報を従来ＰＯＳのキー操作によって入力されていた支払方法の情報と同等に扱い、決済処理に供する。また、制御手段５に、指紋情報読み取り装置、声紋情報読み取り装置、又は顔画像の撮像装置等の生物的情報の読み取り装置を併設し、制御手段５が、決済時の暗証番号の認証だけでなく、指紋認証、声紋認証又は顔認証等の生物的認証を行った上で決済情報の送信を許可してもよい。これにより装置盗難時の安全性を高めることができる。

【００２８】

【発明の効果】本発明は、以上のように構成され機能す

るので、これによると、決済情報をユーザの携帯装置から店舗装置に送信するので、決済の際にクレジットカードを店員に手渡す必要がなく、従来のようにカードに記録された情報が盗まれるおそれが少ない。また、決済情報及び暗証情報を予め記憶させるか又はオンラインで取得させることにより、カード会社は、ユーザにカードを郵送する手間が不要となる。

【００２９】また、請求項２記載の発明では、決済情報を表示手段に表示しないので、決済情報を盗まれて不正使用されるおそれがない。

【００３０】また、請求項３記載の発明では、決済禁止手段を備えたので、ユーザは、従来のカード会社のコールセンターに頼らずに、自分で速やかに決済機能の差し止めができ、コールセンターに連絡を取る手間が不要になると共に、従来より速やかな差し止めが可能となり、不正使用に対する安全性が高まる。また、カード会社のコールセンターは、カードを紛失した会員の対応に追われる手間が不要となり、費用削減を図ることができる、という従来にない優れた決済機能付き通信装置を提供することができる。

＊【図面の簡単な説明】

【図１】本発明の一実施形態の構成を示すブロック図である。

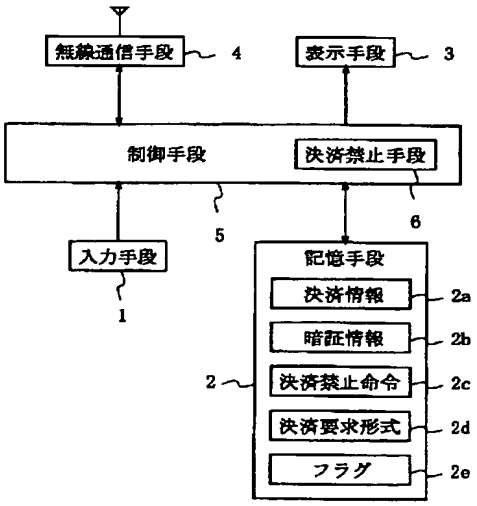
【図２】バーチャルクレジットカード機能のフローチャートである。

【図３】決済機能の不正使用を防止する処理のフローチャートである。

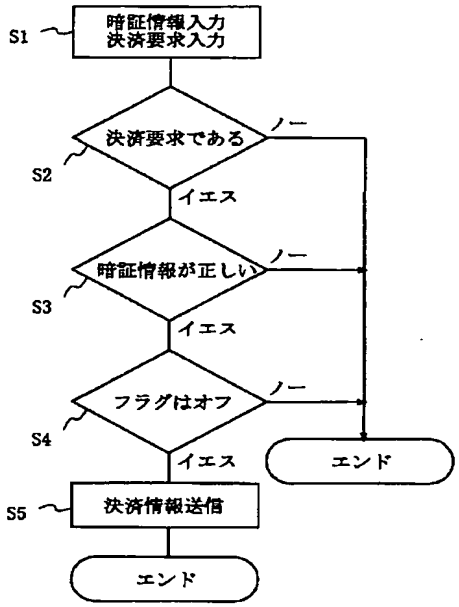
【符号の説明】

１　入力手段
２　記憶手段
２ａ　決済情報記憶手段
２ｂ　暗証情報記憶手段
２ｃ　決済禁止命令記憶手段
２ｄ　決済要求形式記憶手段
２ｅ　フラグ記憶手段
３　表示手段
４　無線通信手段
５　制御手段
６　決済禁止手段

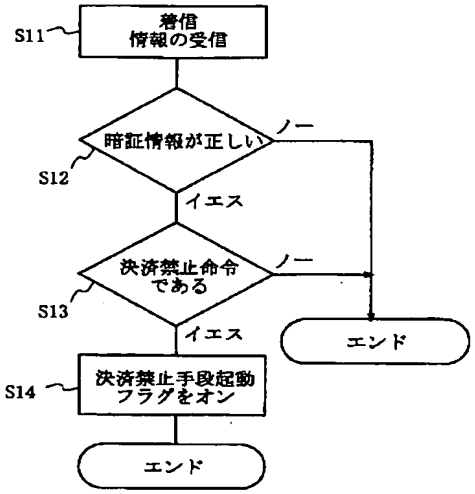
【図１】




【図２】



【図３】




---

フロントページの続き

| (51)Int.Cl.' | 識別記号 | Ｆ Ｉ | テーマコード (参考) |
|---|---|---|---|
| Ｇ０７Ｇ　1/14 | | Ｇ０７Ｆ　7/08 | Ｃ |

(72)発明者　富樫　直記
東京都品川区北品川三丁目３番５号ＴＯＨＯビル　フューチャーフィナンシャルストラテジー株式会社内

Ｆターム(参考)　3E040 AA04 BA18 CA14 CB04 CB05
DA01 DA03 FH01 FH02 FH05
3E042 BA01 BA18 CC03
3E044 AA03 BA04 BA05 CA03 CB01
DA05 DA06 DA10 DB11 DD01
DE01 DE02
5B049 AA02 AA05 BB11 CC36 CC39
DD01 EE21 GG01 GG03 GG06